Acta Sci. Math., 53 (1989), 207—216

Endliche Loops und ihre Unterloopverbände

HUBERTA LAUSCH

Die vorliegende Arbeit setzt die bereits in [8] begonnene Untersuchung endlicher Loops und ihrer Unterloopverbände fort. Auch hier zeigt sich, daß ohne zusätzliche Forderungen an die Struktur der Loops, wie z. B. Potenz- oder Diassoziativität, zentrale Nilpotenz etc., kaum Aussagen darüber möglich sind, welche Auswirkungen die Struktur des Unterloopverbandes auf die Struktur der Loop hat und umgekehrt.

Der erste Abschnitt behandelt endliche Loops mit modularen Unterloopverbänden und gibt eine vollständige Beschreibung von endlichen Loops mit booleschen Unterloopverbänden. Wesentlichstes Ergebnis des zweiten Abschnitts ist, daß endliche Loops mit schwach booleschen Unterloopverbänden von (höchstens) zwei Elementen erzeugt werden können (Satz 2.1). Abschnitt 3 wendet sich den endlichen zentral nilpotenten Loops zu. Beispielsweise erfüllt der Unterloopverband einer endlichen zentral nilpotenten Loop stets die Jordan—Dedekind-Kettenbedingung (Satz 3.1).

Der abschließende Abschnitt 4 ist den endlichen kommutativen Moufang-Loops gewidmet. In Satz 4.1 wird das Resümee aus den bisherigen Ergebnissen über endliche kommutative Moufang-Loops und ihre Unterloopverbände gezogen. Sodann ergibt sich für endliche kommutative Moufang-Loops mit modularen Unterloopverbänden eine interessante Analogie zu den endlichen nilpotenten Gruppen: Eine endliche kommutative Moufang-Loop besitzt genau dann einen modularen Unterloopverband, wenn alle ihre Unterloops quasinormal sind (Korollar 4.4). Ferner erhält man für endliche kommutative Moufang-Loops mit modularen Unterloopverbänden die schöne Strukturausage, daß die Faktorloop $G/Z(G)$ einer derartigen Loop G nach ihrem assoziativen Zentrum $Z(G)$ eine elementar-abelsche 3-Gruppe ist (Satz 4.7). Endliche kommutative Moufang-Loops mit modularen Unterloopverbänden sind also insbesondere nilpotent der Klasse zwei.

Die Bezeichnungen sind im wesentlichen wie in [3] bzw. [5] gewählt; mit $L(G)$ bezeichnen wir den Unterloopverband einer Loop G.

Received June 17, 1986 and in revised form April 11, 1988.

1. Loops mit modularen und booleschen Unterloopverbänden

Für endliche Loops mit modularen Unterloopverbänden kann man keine wirklich schönen Strukturaussagen erwarten, wie bereits die Diskussion spezieller modularer Verbände (projektiver Geometrien) in [8] gezeigt hat. Ganz im Gegensatz zu den Gruppen brauchen endliche Loops mit modularen Unterloopverbänden nicht direkte Produkte von Unterloops zu sein; dies belegen die Beispiele 3.2 und 3.3 in [8]. Doch spielt (ähnlich wie für Gruppen) die Vertauschbarkeit zweier Unterloops einer Loop G eine gewisse Rolle. Zwei Unterloops U, V der Loop G heißen *vertauschbar*, wenn $U \cup V = UV = VU$ gilt, und man nennt eine Unterloop U von G *quasinormal* in G, wenn U mit allen Unterloops von G vertauschbar ist. Auch für Loops hat man die folgende, [11, Theorem 5, p. 5] entsprechende Aussage:

1.1. Satz. *Sind zwei Unterloops U, V der Loop G vertauschbar, so gilt für alle Unterloops $W \supseteq U$ die modulare Identität* $(U \cup V) \cap W = U \cup (V \cap W)$.

Daher besitzen Loops, in denen alle Unterloops quasinormal sind, modulare Unterloopverbände. Insbesondere trifft dies für hamiltonsche Loops zu, in denen alle Unterloops normal, also erst recht quasinormal sind.

Für potenzassoziative p-Loops, wo p eine Primzahl ist, gilt:

1.2. Satz. *Sei G eine potenzassoziative p-Loop. Dann bilden die Elemente der Ordnung p zusammen mit 1 eine charakteristische Unterloop. Ist G sogar diassoziativ, so bilden die Elemente der Ordnung p zusammen mit 1 eine charakteristische kommutative Unterloop.*

Beweis. Seien, $a, b \in G$ zwei Elemente der Ordnung p. Da $L(\langle a, b\rangle)$ wegen der Modularität endliche Länge hat, ist $\langle a, b\rangle$ endlich. Gäbe es ein Element $g \in \langle a, b\rangle$ der Ordnung p^i, $1 < i \in \mathbf{N}$, so wäre $\langle g\rangle \cap \langle a\rangle = \langle g\rangle \cap \langle b\rangle = \langle 1\rangle$. Wegen der Modularität von $L(\langle a, b\rangle)$ müßte $\langle g\rangle = \langle a, b\rangle$ gelten und $\langle a, b\rangle$ wäre zyklische Gruppe. Also hat jedes von 1 verschiedene Element von $\langle a, b\rangle$ die Ordnung p, was die erste Behauptung zeigt. Für diassoziatives G ist $\langle a, b\rangle$ nach [11, Proposition 1.7, p. 14] eine Gruppe der Ordnung p^2, also kommutativ.

Als Folgerung aus dem obigen Satz ergibt sich, daß alle Elemente einer Ordnung $\leqq p^n$, $n \in \mathbf{N}$, einer potenzassoziativen p-Loop G eine charakteristische Unterloop von G bilden.

Nun geben wir eine vollständige Beschreibung endlicher Loops, deren Unterloopverbände boolesch, d. h. distributiv und komplementiert sind. Dazu rekapitulieren wir einige wichtige Ergebnisse aus [8]: Endliche Loops (und alle ihre Unterloops) mit distributiven Unterloopverbänden sind monogen. Als Konsequenz davon sind potenzassoziative Loops mit distributiven Unterloopverbänden zyklische Grup-

pen. Hilfreich ist ferner die Beobachtung, daß die Frattiniunterloop einer Loop mit einem komplementierten Unterloopverband trivial ist, vgl. [11, Proposition 1.14, p. 26]. Falls der Unterloopverband der Loop G die triviale boolesche Algebra ist, sind keine genaueren Aussagen über die Struktur von G möglich, da es für jede ungerade natürliche Zahl $n \geqq 5$ eine Loop der Ordnung n ohne echte Unterloops gibt, s. [5, p. 93 f.]. Zur Vereinfachung der Schreibweise führen wir die folgende Bezeichnung ein: Für Elemente $a_j \in G$, $j \in J$, $J \subseteqq \{1, \ldots, n\}$ bezeichne $\prod_{j \in J} a_j$ das Produkt aller a_j, $j \in J$, in beliebiger Reihenfolge und mit beliebiger Klammerung des Produktes. Damit gilt:

1.3. Satz. *Der Unterloopverband einer Loop G ist genau dann eine boolesche Algebra der Länge n, wenn n Unterloops $A_i = \langle a_i \rangle$, $1 \neq a_i \in A_i$, $i = 1, \ldots, n$, ohne echte Unterloops in G existieren, die paarweise trivialen Durschschnitt haben und für welche gilt:*

(a) $G = \langle A_i | i = 1, \ldots, n \rangle = \langle \prod_{i=1,\ldots,n} a_i \rangle$.

(b) *Für jede Unterloop $\langle 1 \rangle \neq U < G$ gibt es eine geeignete Teilmenge $J \subset \{1, \ldots, n\}$ mit $U = \bigcup_{j \in J} A_j = \langle \prod_{j \in J} a_j \rangle$.*

(c) *Sind $U = \langle \prod_{j \in J} a_j \rangle$ und $V = \langle \prod_{k \in K} a_k \rangle$ mit $J, K \subset \{1, \ldots, n\}$ zwei Unterloops von G, so hat man $U \cup V = \langle \prod_{i \in J \cup K} a_i \rangle$, $U \cap V = \langle \prod_{r \in J \cap K} a_r \rangle$, falls $J \cap K \neq \emptyset$ und $U \cap V = \langle 1 \rangle$ für $J \cap K = \emptyset$.*

Zum Beweis von Satz 1.3 hat man nur zu beachten, daß der Verband aller Teilmengen von $\{1, \ldots, n\}$ eine boolesche Algebra der Länge n ist.

Für potenzassoziative Loops ergibt sich unmittelbar aus [8, Satz 1.2] und [12, Corollary 2]:

1.4. Korollar. *Die endlichen potenzassoziativen Loops mit booleschen Unterloopverbänden sind genau die zyklischen Höldergruppen.*

2. Loops mit schwach booleschen Unterloopverbänden

Der Unterloopverband $L(G)$ einer Loop G heißt *schwach boolesch*, wenn das Intervall $[G/A]$ für jedes Atom A von $L(G)$ boolesch ist. Endliche Loops mit schwach booleschen Unterloopverbänden haben die folgende bemerkenswerte Eigenschaft:

2.1. Satz. *Sei G eine endliche Loop mit schwach booleschem Unterloopverband $L(G)$. Dann ist G von höchstens zwei Elementen erzeugbar.*

Beweis. Falls es in $L(G)$ genau ein Atom gibt, so ist $L(G)$ offensichtlich distributiv und G kann nach [8, Satz 1.2] sogar von nur einem Element erzeugt werden.

Seien nun $A_1, \ldots, A_n$ die Atome von $L(G)$. Falls das Intervall $[G/A_i]$ für alle $i=1, \ldots, n$ die boolesche Algebra der Länge 1 ist, so stellt $L(G)$ eine projektive Gerade dar und wird daher nach [8, Satz 4.1] von höchstens zwei Elementen erzeugt. Ist $[G/A_i]$ für mindestens ein $i \in \{1, \ldots, n\}$ eine boolesche Algebra der Länge $l>1$, so wird G bereits von zwei maximalen Unterloops aus $[G/A_i]$ erzeugt. Sei nun A_i so gewählt, daß $[G/A_i]$ eine boolesche Algebra maximaler Länge in $L(G)$ ist. Das Atom A_i wird offenbar von einem Element erzeugt, sei $A_i=\langle a_i\rangle$, $1 \neq a_i \in A_i$. Nun seien B_j, $j=1, \ldots, m$, die Atome von $[G/A_i]$. Dann ist $L(B_j)$, $j=1, \ldots, m$, entweder eine Kette der Länge zwei und B_j wird von einem Element $b_j \in B_j$, $b_j \notin A_i$, erzeugt, oder B_j ist das Erzeugnis von A_i und einer weiteren Unterloop C von G. Dabei ist C notwendigerweise ein Atom von $L(G)$, denn sonst wäre $[G/A_i]$ keine boolesche Algebra maximaler Länge. Also gilt in jedem Fall $B_j=\langle b_j, a_i\rangle$, $1 \neq b_j \notin A_i$, $j=1, \ldots, m$. Nun ist G aber die Vereinigung aller Atome B_j, $j=1, \ldots, m$, von $[G/A_i]$, also gilt $G=\langle b_j, a_i \mid j=1, \ldots, m\rangle$. Wir betrachten die von dem Produkt $b_1 \ldots b_m$ (mit beliebiger Klammerung) und dem Element a_i erzeugte Unterloop $H=\langle b_1 \ldots b_m, a_i\rangle$ von G. Trivialerweise hat man $A_i < H$. Wäre H eine echte Unterloop von G, so wäre entweder $H=A_i$ oder H wäre Vereinigung von $r<m$ Atomen B_j. In beiden Fällen wäre H also in einer maximalen Unterloop M von G enthalten; o. B. d. A. dürfen wir $H<\langle b_1, \ldots, b_{m-1}, a_i\rangle$ annehmen. Dann folgt $b_1 \ldots b_m \in \langle b_1, \ldots, b_{m-1}, a_i\rangle$, was nach Voraussetzung nicht möglich ist. Daher gilt $H=G$ und die Behauptung ist gezeigt.

Für diassoziative Loops hat Satz 2.1 eine interessante Konsequenz, die eine wesentliche Verallgemeinerung von [10, Korollar 3 in Abschnitt 2] darstellt und die insbesondere für Moufang-Loops gilt:

2.2. Korollar. *Der Unterloopverband einer endlichen diassoziativen Loop G ist genau dann schwach boolesch, wenn G eine Gruppe von einem der folgenden Typen ist:*

(1) *zyklische Höldergruppe,*
(2) $\mathbf{Z}(p^2)$ *für eine Primzahl p,*
(3) $\mathbf{Z}(p) \times \mathbf{Z}(p)$ *für eine Primzahl p,*
(4) *direkt unzerlegbare Höldergruppe mit primzyklischer Kommutatorgruppe.*

Abschließend geben wir noch ein Beispiel für eine nicht diassoziative Loop mit einem schwach booleschen Unterloopverband.

2.3. Beispiel. Die Loop $G=\{1, \ldots, 16\}$ sei gegeben durch die Permutationen (zur Schreibweise s. [8, Abschnitt 3])

$$R_2 = (1\,2)(3\,4)(5\,6)(7\,13\,10\,16\,15\,12)(8\,11)(9\,14),$$
$$R_3 = (1\,3\,2\,4)(5\,10\,14\,16\,12\,11\,9\,13\,7\,6\,8\,15),$$

$$R_4 = (1\,4\,2\,3)(5\,15\,10\,12\,8\,14\,7\,16\,6\,9)(11\,13),$$
$$R_5 = (1\,5\,2\,6)(3\,14\,10\,15\,7\,11)(4\,13\,9\,12\,16\,8),$$
$$R_6 = (1\,6\,2\,5)(3\,15\,9\,11\,10\,4\,16\,7\,12\,13\,14\,8),$$
$$R_7 = (1\,7\,8\,9\,10)(2\,16\,14\,12)(3\,6\,13\,5)(4\,15\,11),$$
$$R_8 = (1\,8\,10\,7\,9)(2\,15\,13\,3\,12\,6\,4\,11\,16\,5\,14),$$
$$R_9 = (1\,9\,7\,10\,8)(2\,12\,3\,11\,15\,14\,13\,6\,16)(4\,5),$$
$$R_{10} = (1\,10\,9\,8\,7)(2\,11)(3\,16\,13\,15\,4\,14\,6)(5\,12),$$
$$R_{11} = (1\,11\,12\,9\,3\,10\,6\,14\,15\,16)(4\,8\,5\,7\,2\,13),$$
$$R_{12} = (1\,12\,15)(2\,16\,13)(3\,5\,8\,16\,4\,9\,6\,7)(11\,14),$$
$$R_{13} = (1\,13\,16\,10\,5\,11\,7\,14)(2\,9\,15\,3\,8)(4\,6\,12),$$
$$R_{14} = (1\,14\,4\,12\,10\,3\,7\,5\,9\,16\,11\,6\,15\,2\,8\,13),$$
$$R_{15} = (1\,15\,8\,6\,10\,11\,5\,16\,9\,2\,14\,3\,13\,12)(4\,7),$$
$$R_{16} = (1\,16\,3\,9\,4\,10\,2\,7\,15\,6\,11)(5\,13\,8\,12\,14).$$

Die Loop G besitzt die Unterloops $A_1=\{1, 2\}$, $A_2=\{1, 7, 8, 9, 10\}$, $B_1=\{1, 2, 3, 4\}$, $B_2=\{1, 2, 5, 6\}$. Dabei sind A_1 und A_2 die Atome von $L(G)$; das Intervall $[G/A_1]$ ist eine boolesche Algebra der Länge 2, das Intervall $[G/A_2]$ eine boolesche Algebra der Länge 1. Ferner gilt $G=\langle A_1, A_2\rangle=\langle B_1, B_2\rangle=\langle B_1, A_2\rangle=\langle B_2, A_2\rangle$. Außerdem kann G von nur einem Element erzeugt werden, man hat nämlich $G=\langle 11\rangle=\langle 12\rangle=$ $=\langle 13\rangle=\langle 14\rangle=\langle 15\rangle=\langle 16\rangle$.

3. Zentral nilpotente endliche Loops

Im folgenden Abschnitt 4 werden wir uns mit endlichen kommutativen Moufang-Loops beschäftigen. Da endlich erzeugte kommutative Moufang-Loops zentral nilpotent sind (s. [5, Theorem 10.1, p. 157]), lohnt es sich, zunächst endliche zentral nilpotente Loops zu untersuchen.

Bekanntlich erfüllt der Untergruppenverband $L(G)$ einer endlichen Gruppe G genau dann die Jordan—Dedekind-Kettenbedingung, wenn G überauflösbar ist. Daher erfüllen insbesondere die Untergruppenverbände endlicher nilpotenter Gruppen die Jordan—Dedekind-Kettenbedingung. Für endliche zentral nilpotente Loops hat man die entsprechenden Sätze wie für endliche nilpotente Gruppen, da die Ordnung jeder Unterloop die Ordnung jeder sie enthaltenden Unterloop teilt. Ferner ist eine Unterloop einer zentral nilpotenten Loop G genau dann maximal in G, wenn sie normal in G ist und Primzahlindex in G hat, s. [4, Theorem 7B, Lemma 7F + Corollary]. Weiter existiert stets eine Hauptreihe $G=A_0\supset A_1\supset\ldots\supset A_r=\langle 1\rangle$,

wobei jede Faktorloop A_{i-1}/A_i keine echten Unterloops besitzt und A_i Primzahlindex in A_{i-1} hat. Daher folgt mit genau den gleichen Argumenten wie für Gruppen (vgl. [3, p. 177] und [11, Theorem 9, p. 9]):

3.1. Satz. *Der Unterloopverband einer endlichen zentral nilpotenten Loop erfüllt die Jordan—Dedekind-Kettenbedingung.*

Ferner gestatten endliche zentral nilpotente Loops noch die folgenden Aussagen:

3.2. Satz. *Eine endliche zentral nilpotente Loop G hat genau dann einen komplementierten Unterloopverband $L(G)$, wenn G ein direktes Produkt elementar-abelscher p-Gruppen ist.*

Beweis. Da G endlich ist, ist die Frattiniunterloop $\Phi(G)$ von G verschieden von G und wegen der Komplementiertheit von $L(G)$ gilt $\Phi(G)=\langle 1\rangle$. Daher ist G nach [5, Theorem 2.2, p. 98] eine abelsche Gruppe und mit [11, Proposition 1.15, p. 16] folgt nun die Behauptung.

Aus Satz 3.2 und [8, Satz 1.2] ergibt sich unmittelbar:

3.3. Korollar. *Ist der Unterloopverband einer endlichen zentral nilpotenten Loop G eine boolesche Algebra, so ist G eine zyklische Höldergruppe.*

Als weitere Folgerung aus Satz 3.2 erhält man mit Hilfe von [12, Corollary of Theorem 1]:

3.4. Korollar. *Der Unterloopverband $L(G)$ einer endlichen zentral nilpotenten Loop G ist genau dann orthomodular, wenn G direktes Produkt von P-Gruppen mit paarweise teilerfremden Ordnungen ist.*

4. Endliche kommutative Moufang-Loops

In den vorhergehenden Abschnitten haben wir gesehen, daß man für endliche kommutative Moufang-Loops und ihre Unterloopverbände einige schöne Aussagen machen kann. Dies rechtfertigt eine gesonderte Behandlung endlicher kommutativer Moufang-Loops. Zunächst seien hier noch einmal die wichtigsten Ergebnisse zusammengestellt.

4.1. Satz. *Für eine endliche kommutative Moufang-Loop G mit dem Unterloopverband $L(G)$ gelten:*

(1) *$L(G)$ erfüllt die Jordan—Dedekind-Kettenbedingung.*

(2) *$L(G)$ distributiv $\Leftrightarrow$ G zyklische Gruppe.*

(3) *$L(G)$ komplementiert $\Leftrightarrow$ G direktes Produkt elementar-abelscher p-Gruppen.*

(4) *$L(G)$ boolesch $\Leftrightarrow$ G zyklische Höldergruppe.*

(5) *$L(G)$ schwach boolesch $\Leftrightarrow$ G ist abelsche Gruppe von genau einem der folgenden Typen: zyklische Höldergruppe, $\mathbf{Z}(p^2)$, $\mathbf{Z}(p)\times\mathbf{Z}(p)$.*

Im folgenden soll die Struktur von endlichen kommutativen Moufang-Loops mit modularen Unterloopverbänden hergeleitet werden. Es zeigt sich, daß für endliche kommutative Moufang-Loops — ähnlich wie für endliche nilpotente Gruppen, vgl. [11, Theorem 8, p. 8] — die Umkehrung von Satz 1.1 gilt. Dazu benötigen wir zunächst das folgende Lemma.

4.2. Lemma. *Die Unterloops U und V einer endlichen kommutativen Moufang-Loop G sind genau dann vertauschbar, wenn $|(U\cup V)\colon U|=|V\colon (U\cap V)|$ gilt.*

Beweis. Sei zunächst $|(U\cup V)\colon U|=|V\colon (U\cap V)|$. Dann gilt $|U\cup V|=|U|\cdot|(U\cup V)\colon U|=|U|\cdot|V\colon (U\cap V)|=|UV|=|VU|$, woraus wegen $UV=VU\subseteqq\langle U,V\rangle$ sofort $U\cup V=UV=VU$ folgt. Seien nun U und V vertauschbar. Dann hat man $|U\cup V|=|UV|=|U|\cdot|V\colon (U\cap V)|$ und andererseits $|U\cup V|=|(U\cup V)\colon U|\cdot|U|$. Damit folgt die behauptete Identität.

Jetzt können wir den gewünschten Satz zeigen:

4.3. Satz. *Sei G eine endliche kommutative Moufang-Loop und seien U und V ein modulares Paar von Unterloops von G. Dann sind U und V vertauschbar.*

Beweis. Als endliche kommutative Moufang-Loop ist G direktes Produkt einer endlichen abelschen Gruppe A von zu 3 teilerfremder Ordnung und einer kommutativen 3-Moufang-Loop B. Daher läßt sich G als direktes Produkt der p-Sylowgruppen $S_1, \ldots, S_n$ von A und der 3-Moufang-Loop B schreiben, also $G=S_1\times\ldots\times S_n\times B$, s. [7, Proposition 1.3]. Somit ist auch jede Unterloop U von G in der Form $U=U_1\times\ldots\times U_n\times U_{n+1}$ mit $U_i=U\cap S_i$ $(i=1,\ldots,n)$, $U_{n+1}=U\cap B$ darstellbar. Seien also $U=U_1\times\ldots\times U_{n+1}$ und $V=V_1\times\ldots\times V_{n+1}$ ein modulares Paar von Unterloops von G. Wir bezeichnen die Ordnungen von $U, V, U\cup V, U\cap V, U_i, V_i, U_i\cup V_i$ bzw. $U_i\cap V_i$ mit $u, v, m, d, u_i, v_i, m_i$ bzw. d_i. Wegen $U\cup V=(U_1\cup V_1)\times\ldots\times(U_{n+1}\cup V_{n+1})$ folgt $m=\prod_{i=1}^{n+1} m_i$ und $d=\prod_{i=1}^{n+1} d_i$, und md ist durch uv teilbar. Andererseits wird das Intervall $[(U\cup V)/U]$ von $L(G)$ wegen der Gültigkeit der modularen Identität isomorph auf das Intervall $[V/(U\cap V)]$ abgebildet. Da G zentral nilpotent ist, sind auch $U, V, U\cup V$ und $U\cap V$ zentral nilpotent und es existiert je eine Hauptreihe zwischen $U\cup V$ und U sowie zwischen V und $U\cap V$, s. [4, Abschnitt 7]; dabei ist die Länge einer Hauptreihe zwischen $U\cup V$ und U nicht größer als die Länge einer Hauptreihe zwischen V und $U\cap V$. Daher ist die Anzahl der Primfaktoren in $|(U\cup V)\colon U|=m/u$ nicht größer als die Anzahl der Primfaktoren in $|V\colon (U\cap V)|=v/d$. Wegen $uv|md$ muß $md=uv$, also $|(U\cup V)\colon U|=|V\colon (U\cap V)|$ gelten. Nach Lemma 4.2 hat man somit $U\cup V=\langle U,V\rangle=UV=VU$.

Aus den Sätzen 4.3 und 1.1 folgt unmittelbar:

4.4. Korollar. *Eine endliche kommutative Moufang-Loop besitzt genau dann einen modularen Unterloopverband, wenn alle ihre Unterloops quasinormal sind.*

Eine wichtige Klasse von Loops, in denen alle Unterloops quasinormal sind, sind die hamiltonschen Loops. Wegen der Diassoziativität von Moufang-Loops ergibt sich mit [5, Theorem 7.2, p. 87] sofort, daß endliche hamiltonsche kommutative Moufang-Loops abelsche Gruppen sind. Von besonderem Interesse ist daher die Struktur nicht hamiltonscher kommutativer Moufang-Loops mit modularen Unterloopverbänden, die im folgenden untersucht wird.

4.5. Lemma. *Sei $G=A\times B$ eine endliche kommutative Moufang-Loop mit einer abelschen Gruppe A von zu 3 teilerfremder Ordnung und einer kommutativen 3-Moufang-Loop B. Dann ist der Unterloopverband $L(G)$ von G genau dann modular, wenn $L(B)$ modular ist.*

Beweis. Wegen [5, p. 101] ist G in der angegebenen Form $G=A\times B$ darstellbar und mit $L(G)$ ist auch $L(B)$ modular. Da $L(A)$ als Untergruppenverband einer abelschen Gruppe von vornherein modular ist, ist umgekehrt für die Modularität von $L(G)$ die Modularität von $L(B)$ hinreichend (vgl. den Beweis von Theorem 4, p. 5, in [11]).

Somit können wir uns darauf beschränken, endliche kommutative 3-Moufang-Loops mit modularen Unterloopverbänden zu untersuchen. Ein wichtiges Hilfsmittel dazu liefert das folgende Lemma:

4.6. Lemma. *Eine kommutative 3-Moufang-Loop B vom Exponenten 3 hat genau dann einen modularen Unterloopverband, wenn B eine elementar-abelsche 3-Gruppe ist.*

Beweis. Angenommen, B ist keine Gruppe. Dann gibt es unter den von drei Elementen erzeugten Unterloops mindestens eine nicht assoziative Unterloop $U=\langle x, y, z\rangle$ von B. Wegen [7, Lemma 1.6] hat U mindestens die Ordnung 81, während das Komplexprodukt $\langle x, y\rangle\langle z\rangle$ von der Ordnung 27 ist. Daher kann $L(B)$ nach Korollar 4.4 nicht modular sein.

Das vorstehende Lemma zeigt insbesondere, daß die von allen Elementen der Ordnung 3 erzeugte Unterloop S einer endlichen kommutativen Moufang-Loop G mit modularem Unterloopverband eine elementar-abelsche 3-Gruppe ist, da wegen der Gültigkeit von $(xy)^3=x^3y^3$ für alle $x, y\in G$ alle Elemente $\neq 1$ von S die Ordnung 3 haben. Eine weitaus wichtigere Konsequenz aus Lemma 4.6 ist jedoch die folgende Aussage:

4.7. Satz. *Es sei G eine endliche kommutative Moufang-Loop und $Z(G)$ ihr assoziatives Zentrum. Ist der Unterloopverband $L(G)$ von G modular, so ist die Faktorloop $G/Z(G)$ eine elementar-abelsche 3-Gruppe. Insbesondere ist G also nilpotent der Klasse 2.*

Beweis. Nach [9, Theorem 1.8, p. 9] ist $G/Z(G)$ eine kommutative Moufang-Loop vom Exponenten 3. Da mit $L(G)$ auch $L(G/Z(G))$ modular ist, muß $G/Z(G)$ wegen Lemma 4.6 eine abelsche Gruppe vom Exponenten 3 sein.

Übrigens hat Satz 4.7 eine interessante Parallele für endliche Gruppen mit modularen Untergruppenverbänden, sogenannte M-Gruppen: Endliche M-Gruppen sind stets metabelsch, s. [11, Theorem 15, p. 18].

Das kleinste Beispiel für eine nicht assoziative kommutative 3-Moufang-Loop mit modularem Unterloopverband ist die von den Elementen x, y, z mit den definierenden Relationen $x^3=y^3=z^9=1$, $(x, y, z)=z^3$ erzeugte Loop B der Ordnung 81, s. [7, Proposition 6.1]: Alle echten Unterloops von B sind Gruppen, also ist das Komplexprodukt zweier Unterloops, die zusammen eine echte Unterloop von B erzeugen, gleich dem Erzeugnis dieser Unterloops; das Komplexprodukt zweier Unterloops, deren Erzeugnis B ist, hat die Ordnung 81 und ist daher gleich B. Somit sind alle Unterloops von B quasinormal.

Literaturverzeichnis

[1] A. A. Albert, Quasigroups. I, *Trans. Amer. Math. Soc.*, **54** (1943), 507—519; II, *Trans. Amer. Math. Soc.*, **55** (1944), 401—419.

[2] L. Bénéteau, L'irréductibilité centrale dans les boucles de Moufang commutatives et dans systèmes triples de Hall, *Discrete Math.*, **45** (1983), 31—44.

[3] G. Birkhoff, *Lattice Theory*, Colloq. Publ., Vol. XXV., Amer. Math. Soc. (Providence, Rhode Island, 3rd ed., 1967).

[4] R. H. Bruck, Contributions to the theory of loops, *Trans. Amer. Math. Soc.*, **60** (1946), 245—354.

[5] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag (Berlin—Heidelberg, 1958).

[6] M. Hall, *The Theory of Groups*, Chelsea (New York, 1976).

[7] T. Kepka, P. Němec, Commutative Moufang Loops and Distributive Groupoids of Small Orders, *Czechoslovak Math. J.*, **31** (1981), 633—669.

[8] H. Lausch, Loops mit distributiven und geometrischen Unterloopverbänden, *J. Geom.*, **26** (1986), 62—76.

[9] Yu. I. Manin, *Cubic Forms*, North Holland, American Elsevier (Amsterdam—London—New York, 1974).

[10] P. Plaumann, K. Strambach, G. Zacher, Gruppen mit geometrischen Abschnitten im Untergruppenverband, *Monatsh. Math.*, **99** (1985), 117—145.

[11] M. SUZUKI, *Structure of a Group and the Structure of its Lattice of Subgroups*, Springer-Verlag (Berlin—Göttingen—Heidelberg, 1956).

[12] G. WHITSON, Finite groups whose subgroup, composition subgroup, or normal subgroup lattice is an ortholattice, *Algebra Universalis*, **8** (1978), 123—127.

MATHEMATISCHES INSTITUT
UNIVERSITÄT WÜRZBURG
AM HUBLAND
8700 WÜRZBURG, WEST GERMANY